JFW
AF

PTO/SB/21 (04-07)
Approved for use through 09/30/2007. OMB 0651-0031
U.S. Patent and Trademark Office: U.S. DEPARTMENT OF COMMERCE
Under the Paperwork Reduction Act of 1995, no persons are required to respond to a collection of information unless it displays a valid OMB control number.

TRANSMITTAL FORM

(to be used for all correspondence after initial filing)

Application Number	10/737,389
Filing Date	December 16, 2003
First Named Inventor	En-Yi Liao
Art Unit	2141
Examiner Name	Serrao, Ranodhi N

Total Number of Pages in This Submission	19	Attorney Docket Number	10033.000400

ENCLOSURES *(check all that apply)*

☐ Fee Transmittal Form
  ☐ Fee Attached
☐ Amendment / Reply
  ☐ After Final
  ☐ Affidavits/declaration(s)
☐ Extension of Time Request
☐ Express Abandonment Request
☐ Information Disclosure Statement
☐ Certified Copy of Priority Document(s)
☐ Reply to Missing Parts/ Incomplete Application
  ☐ Reply to Missing Parts under 37 CFR1.52 or 1.53

☐ Drawing(s)
☐ Licensing-related Papers
☐ Petition
☐ Petition to Convert to a Provisional Application
☐ Power of Attorney, Revocation Change of Correspondence Address
☐ Terminal Disclaimer
☐ Request for Refund
☐ CD, Number of CD(s) _____
  ☐ Landscape Table on CD

☐ After Allowance Communication to TC
☐ Appeal Communication to Board of Appeals and Interferences
☒ Appeal Communication to TC **(Appeal Notice, Brief, Reply Brief)**
☐ Proprietary Information
☐ Status Letter
☒ Other Enclosure(s) *(please identify below)*:
Substitute Second Appeal Brief Filed Under 37 C.F.R. § 41.37 (14 pgs);
Claims Appendix (2 pgs);
Evidence Appendix (1 pg);
Related Proceedings Appendix (1 pg);
Return Receipt Postcard

Remarks

SIGNATURE OF APPLICANT, ATTORNEY, OR AGENT

Firm	OKAMOTO & BENEDICTO LLP
Signature	*Patrick Ben*
Printed Name	Patrick D. Benedicto
Date	July 19, 2007	Reg. No.	40,909

CERTIFICATE OF TRANSMISSION/MAILING

I hereby certify that this correspondence is being facsimile transmitted to the USPTO or deposited with the United States Postal Service with sufficient postage as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below.

Signature	*Patrick Ben*		
Typed or printed name	Patrick D. Benedicto	Date	July 19, 2007

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:

       En-Yi Liao

Application No.:	10/737,389	Examiner:	Serrao, Ranodhi N.
Filing Date:	December 16, 2003	Art Unit:	2141

Assignee: Trend Micro Incorporated

Title: Technique For Intercepting Data In A Peer To Peer Network

---

Honorable Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

SUBSTITUTE SECOND APPEAL BRIEF FILED UNDER 37 C.F.R. § 41.37

Sir:

This substitute appeal brief follows the Notice of Appeal filed by Applicants on May 9, 2007, and is responsive to the Notification of Non-Compliant Appeal Brief mailed June 29, 2007.

This is the second appeal brief filed in this application. The first appeal brief, filed on February 16, 2006, did not reach the Board of Patent Appeals and Interferences (the "Board") as it resulted in issuance of another office action. Therefore, it is believed that no additional fee is required. If for any reason additional fees are required, the Commissioner is hereby authorized to charge the insufficiency to Deposit Account No. 50-2427.

I.   REAL PARTY IN INTEREST

The real party in interest is Trend Micro Incorporated, which is the assignee of the present application.

II.   RELATED APPEALS AND INTERFERENCES

On information and belief, there are no appeals, interferences, or judicial proceedings known to the appellant, the appellant's legal representative, or assignee which may be related to, directly affect or be directly affected by or have a bearing on the Board's decision in the pending appeal.

III.   STATUS OF CLAIMS

Claims 1-9 and 16-21 have been canceled.

Claims 10-15 and 22 are pending in this application and stand rejected.

Claims 10-15 and 22 are involved in the appealed. These claims are rejected in the final office action mailed March 30, 2007 ("final office action").

IV.   STATUS OF AMENDMENTS

No amendment has been filed after the final office action.

V.   SUMMARY OF CLAIMED SUBJECT MATTER

The claimed subject matter relates to interception of data in a peer to peer network. In a conventional peer-to-peer network, data transfer between two peer computers ("peer nodes") are performed directly between the peer computers. This direct data transfer may result in the spread of computer viruses, for example. To address problems relating to peer-to-peer data transfers, embodiments of the invention allow for redirection of data

from a sender peer node to an interception node, where the data can be processed (e.g., scanned for viruses) in-transit to the destination peer node.

Independent claim 10 recites a method of transferring a file in a peer-to-peer computer network (see Specification, FIG. 3, file transfer between peer nodes 110-1 and 110-2 through interception node 330). A file originally intended to be transferred directly (Specification, page 11, lines 3-5; page 15, lines 10-17) from a first peer node to a second peer node is redirected from the first peer node to an interception node (Specification, page 11, lines 12-19; page 12, lines 7-11), where it is processed (Specification, page 12, lines 11-12) prior to being transferred to the second peer node (Specification, page 12, lines 12-13).

Independent claim 22 recites a method of transferring a file in a peer-to-peer computer network (see Specification, FIG. 3, data transfer between peer nodes 110-1 and 110-2 through interception node 330). A file originally intended to be transferred directly (Specification, page 11, lines 3-5; page 15, lines 10-17) from a first peer node to a second peer node is first transferred to an interception node (Specification, page 11, lines 12-19; page 12, lines 7-11), where the file is scanned for viruses (Specification, page 10, lines 16-19; page 12, lines 11-12) prior to being transferred to the second node (Specification, page 12, lines 12-13).

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

The following are to be reviewed on appeal:

1.   The rejection of claims 10-14 and 22 under 35 U.S.C. § 103(a) as being unpatentable over U.S. 5,781,550 to Templin et al. ("Templin") and U.S. Publication No. 2004/0158741 by Schneider ("Schneider").

2.   The rejection of claim 15 under 35 U.S.C. § 103(a) as being unpatentable over Templin and Schneider as applied to claim 10, and further in view of U.S. Patent No. 6,629,100 to Morris et al. ("Morris").

VII. ARGUMENTS

Applicants traverse the rejection of claims 10-15 and 22 for the following reasons.

A.   CLAIMS 10-13

Claims 10-13 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over U.S. 5,781,550 to Templin et al. ("Templin") and U.S. Publication No. 2004/0158741 by Schneider ("Schneider"). The rejection is respectfully traversed.

There are three requirements to establish a prima facie case of obviousness. First, there must be some suggestion or motivation to modify a reference or to combine references. Second, there must be a reasonable expectation of success. Third, the prior art reference or combined references must teach or suggest all the claim limitations. See MPEP § 2143.

The plain language of claim 10 requires redirection of a file involved in a peer-to-peer transfer from a first peer node to an interception node, and then transfer of the file from the interception node to a second peer node. The file is originally intended to be transferred directly from the first peer node to the second peer node as is consistent with peer-to-peer transfer.

1.   The combination of Templin and Schneider does not teach or suggest redirection of files involved in a peer-to-peer data transfer.

Claim 10 is patentable over the combination of Templin and Schneider at least for reciting: "redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node" (emphasis added).

As noted in the final office action, Templin does not teach file transfer in a peer-to-peer computer network. This is not surprising given that Templin pertains to a computer gateway. Templin FIG. 1 is reproduced below for ease of discussion.

FIG. I
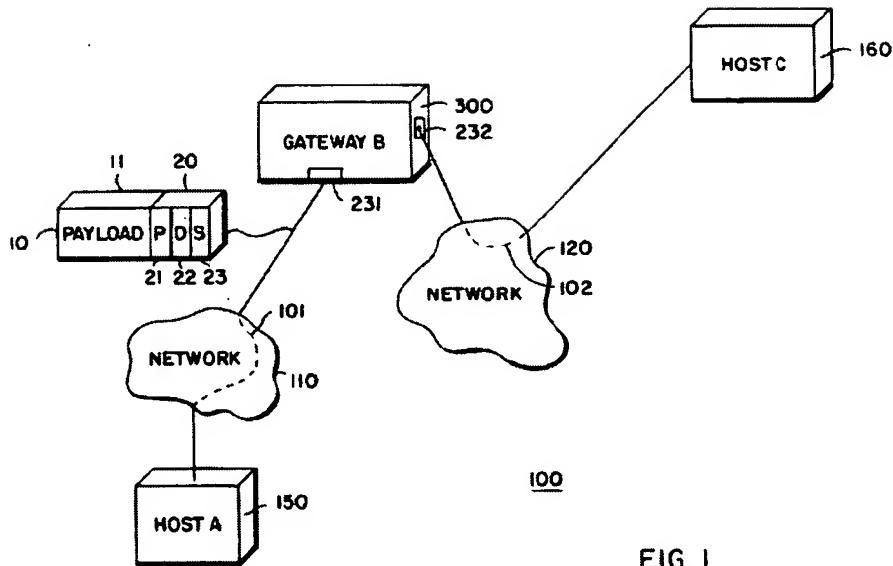
As shown in Templin FIG. 1, Templin's gateway 300 connects network 110 to network 120 (Templin, col. 3, line 66 to col. 4, line1). As is conventional with gateway architectures, data being transferred between computer 150 and computer 160 must physically pass through the interfaces 231 and 232 of the gateway 300 (Templin, col. 5, lines 12-15). That is, the gateway 300 receives all data being transferred between networks 110 and 120 because of its centralized gate keeping location. This is also evident in Templin, col. 3, lines 21-31, which describes that the destination address of packets received in the gateway 300 is that of the destination computer, not that of the gateway 300. In other words, the gateway 300 receives data by interception, not redirection as required by claim 10.

The final office action reads Templin's proxy servers 340 as interception nodes (final office action, paragraph 2). There are at least two problems with this claim construction. Firstly, the term "node" in the context of computer networks is well known and refers to a device connected to a network. A node is not a process running in a computer, although the computer itself may be a node. There is no dispute that a proxy server 340 in Templin is a process, i.e., software, executing in the gateway 300.

"The packets can be diverted to proxy servers 340 <u>executing on the gateway 300</u>."
(Templin, col. 5, lines 17-18)

Templin FIG. 3, which shows a flow diagram of the gateway 300 (see Brief Description of the Drawings), evidences that the proxy servers 340 as a software component of the gateway 300. Therefore, a proxy server 340 is definitely not a node, but a process executing on a node, which in this case is the gateway 300.

Secondly, a claim construction that a process executing on the gateway 300 can be an interception node does not make sense when read in light of the rest of the claims. For example, claim 22 recites "scanning the file for viruses <u>in the interception node</u>" (emphasis added). Applicant respectfully submits that there is simply no support for the suggestion that virus scanning can be performed in a proxy server process. As another example, claim 12 depends on claim 10 and recites "wherein processing the file in the interception node comprises scanning the file for viruses." It is respectfully submitted that a proxy server 340 is a process, and thus cannot execute antivirus scanning <u>in it</u>, as would be required if the proxy server 340 is read as interception node. The final office action is thus based on an improper claim construction.

Therefore, it is respectfully submitted that claim 10 is patentable over the combination of Templin and Schneider.

2.   <u>The combination of Templin and Schneider does not teach or suggest processing a file being transferred between two peer nodes in a peer-to-peer data transfer.</u>

The plain language of claim 10 requires "transferring the file from the interception node to the second peer node." As explained above, Templin does not even pertain to peer-to-peer networks. The final office action suggests that Schneider discloses peer-to-peer networks and that it would have been obvious to modify Templin "to a method of transferring a file in a peer-to-peer computer network." The Applicant respectfully disagrees with this conclusion.

Schneider FIG. 1 is reproduced below for ease of discussion.
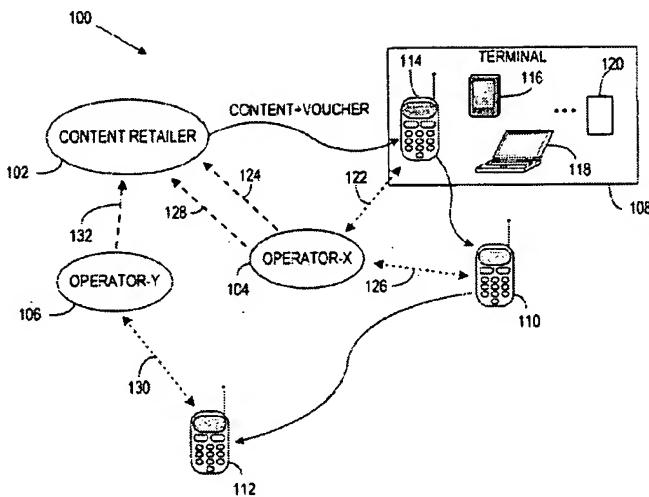
FIG. 1

In Schneider, peer-to-peer data transfer may be performed between terminals 108, 110, and 112. Prior to the peer-to-peer data transfer, data may first be transferred to the operator-X 104 or operator-X 106. This allows virus infected data to be quarantined within the terminal 108, 110, and 112 (Schneider, paragraph 37). Note, however, that the peer-to-peer data transfer itself is still directly between two terminals. That is, the peer-to-peer data transfer is still from one terminal to another (see arrows between terminals). This is conventional peer-to-peer data transfer and does not involve processing of files sent from one terminal to another. Data transfer between terminals is direct as expected of peer-to-peer networks.

In conclusion, Templin pertains to gateways, not peer-to-peer computer networks. Templin does not teach or suggest processing data being transferred from one peer node to another peer node in a peer-to-peer data transfer. Schneider pertains to peer-to-peer computer networks. However, like Templin, Schneider does not teach or suggest processing data being transferred from one peer node to another peer node in a peer-to-peer data transfer. As Schneider proves, conventional peer-to-peer data transfer does not involve processing of data in the middle of the peer-to-peer transfer. Since neither Templin nor Schneider teaches or suggests processing of data involved in a peer-to-peer data transfer, it is respectfully submitted that their combination cannot possibly read on

claim 10. Processing of data in a peer-to-peer data transfer is only taught in the present application, not in any of the references of record.

The final office action suggests that in Schneider it is "clear that the processing of data takes in between the peer nodes" (final office action, paragraph 3), citing to Schneider paragraphs 37, 27, and 38. Applicant respectfully disagrees with this conclusion.

Schneider paragraph 37 discusses using a download server to scan superdistributed content that is transferred between terminals. However, this paragraph does not state that the content transferred between terminals is scanned in the middle of the transfer. Being an intermediary between terminals does not require scanning in transit as the final office action seems to be deducing from paragraph 37. Paragraph 27 talks about forwarding the content to a virus scanning company prior to the consumer's "receipt." It is respectfully submitted that the final office action reads too much in this sentence because it is possible to scan the content prior to a consumer receiving it even when the content is not scanned in-transit between terminals. As evidenced in Schneider FIG. 5, a terminal can have a network server 510 scan the content before transfer (i.e., not in transit between terminals in peer-to-peer) of the content to other terminals for receipt by a consumer.

Paragraph 38 discusses forwarding clean content to the DRM agent of the receiving terminal. However, this doesn't necessarily mean the scanning is performed in transit. This is because forwarding clean content to the DRM agent of the receiving terminal occurs after the forwarding terminal has first outsourced the scanning by forwarding the content to an operator, receiving the content from the operator, and then forwarding the content to the receiving terminal. That is the transfer of clean content occurs between the forwarding and the receiving terminal, not between the operator (or outsourcing server) and the receiving terminal.

Virus scanning in Schneider is explained in detail in FIG. 5, which is reproduced below for each of discussion.
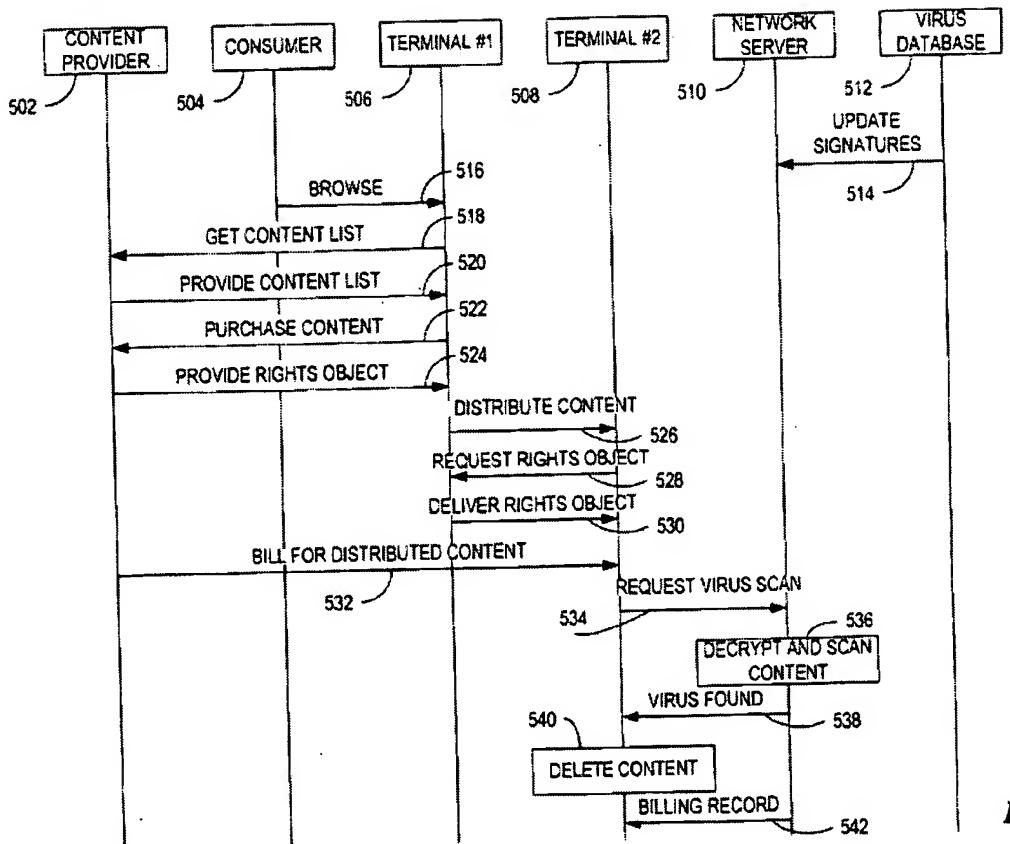
FIG. 5

As shown in Schneider FIG. 5, virus scanning in Schneider is performed in a network server 510 (see arrows 534, 536, and 538). This occurs between a terminal (terminal 508 in the example) and the network server 510, <u>not between terminals as the final office action suggests</u>. As shown in Schneider FIG. 5, there is no virus scanning in-transit between terminals 508 and 506.

Therefore, it is respectfully submitted that claim 10 is patentable over the combination of Templin and Schneider.

3.   <u>There is no motivation to combine Templin and Schneider</u>

Claim 10 is also patentable over the combination of Templin and Schneider because there is no motivation to combine their teachings in the manner suggested in the final office action.

According to the final office action, one of ordinary skill in the art would be motivated to modify Templin to a method of transferring a file in a peer-to-peer computer network "in order to control communication content between two terminals, and more particularly control the proliferation of virus infected content by outsourcing virus scanning services," citing to Schneider paragraph 1. It is respectfully submitted that outsourcing of virus scanning services in Schneider involves doing the scanning using another computer prior to the peer-to-peer data transfer between terminals. As applied to Templin, this would result in the data being processed for virus scanning before the data is even transferred from the computer 150 to the computer 160 by way of the gateway 300. Schneider teaches scanning of content before, not in the middle of, a peer to peer transfer as Schneider is merely performing conventional peer to peer transfer. Scanning content for viruses in the middle of a peer to peer data transfer is taught only in the present application, not in Schneider or any of the references of record.

Furthermore, Templin pertains to data transfer by proxy, which is opposite to that of peer-to-peer. One is a replacement for the other. In Templin, the gateway 300 serves as a proxy in a data transfer between two computers (Templin, col. 3, lines 21-31). As is conventional with proxies, the gateway 300 uses its address to communicate with the other computer. In other words, the gateway running the proxy communicates with one computer, serving as a proxy for another. Peer-to-peer, on the other hand, involves direct data transfer between two computers. Modifying Templin to perform peer-to-peer data transfer would necessarily require removal of the proxy function of Templin's gateway 300, making the gateway 300 unsuitable for its intended use.

The last office action bases its motivation to combine on an incorrect assumption that Schneider discloses virus scanning in a peer-to-peer data transfer between terminals (final office action, paragraph 4). As explained above, Schneider does not disclose virus scanning of content in-transit between peer-to-peer terminals. In Schneider, virus scanning is not in the middle of a peer-to-peer data transfer, but rather before the peer-to-peer data transfer between terminals takes place (e.g., see Schneider FIG. 5).

For at least the above reasons, it is respectfully submitted that claim 10 is patentable over the combination of Templin and Schneider.

Claims 11-13 depend on claim 10. Therefore, it is respectfully submitted that claims 11-13 are patentable over the combination of Templin and Schneider at least for the same reasons that claim 10 is patentable.

B.   CLAIM 22

Claim 22 stands rejected under 35 U.S.C. § 103(a) as being unpatentable over Templin and Schneider ("Schneider"). The rejection is respectfully traversed.

Claim 22 is patentable over the combination of Templin and Schneider at least for the same reasons given for claim 1.

Claim 22 is further patentable over the combination of Templin and Schneider for reciting: "scanning the file for viruses in the interception node."

As noted in the final office action, Templin does not disclose virus scanning in an interception node. However, the final office action suggests that Schneider does. The final office action reads a process server 340 executing on a gateway 300 of Templin as an interception node. This requires Schneider's virus scanning, which is off-loaded to a network server in the network, to execute in the process server of Templin. It is respectfully submitted that this is not feasible given that the interception node, Templin's proxy server, is piece of software providing a proxy function and thus cannot execute virus scanning in it.

C.   CLAIM 14

Claim 14 is patentable over the combination of Templin and Schneider at least for reciting: "informing the second peer node that an address of the first peer node is that of the interception node." According to the final office action, Templin discloses this limitation in col. 3, lines 21-31.

> The gateway receives a packet having a source address of the trusted computer, a destination address, and a first payload. The packet, according to rules stored in a configuration database, is intercepted and diverted to a proxy server of the gateway if the destination address references an untrusted computer. The proxy

server extracts the payload from the packet, and generates a new packet having a source address of the gateway, <u>the destination address of the untrusted computer,</u> and the payload. As an advantage of the invention, this enables the trusted computer to securely communicate with the untrusted computer.

Templin, col. 3, lines 21-31 (emphasis added)

As is explicit from the cited portion of Templin, the packets received by the gateway contain the source address of the trusted computer and, more importantly, the destination address of the untrusted computer. That is, the packets are not redirected to the gateway by informing the trusted computer that the address of the untrusted computer is that of the gateway, as would be required to read on claim 14. This is not surprising given that Templin's gateway does not even perform redirection. Templin's gateway intercepts packets by simply being deployed in-line with the data transfer path.

The final office action suggests that "Since an untrusted computer serves as the second node and a proxy server serves as the interception node, Templin clearly teaches claim 14" (final office action, paragraph 5). The problem with construing Templin's proxy server as an interception node has already been explained above, so claim 14 must be patentable over the combination of Templin and Schneider.

Therefore, it is respectfully submitted that claim 14 is patentable over the combination of Templin and Schneider.

D.   CLAIM 15

Claim 15 stands rejected under 35 U.S.C. § 103(a) as being unpatentable overt Templin and Schneider as applied to claim 10, and further in view of U.S. Patent No. 6,629,100 to Morris et al. ("Morris"). The rejection is respectfully traversed.

Claim 15 recites the method of transferring the file from the interception node to the second peer node. According to the plain language of claim 15, this is performed by "querying a P2P server for location information of peer nodes involved in a transfer of the file" and "based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node."

As noted in the final office action, neither Templin nor Schneider teaches querying a P2P server in transferring the file from the interception node to the second peer node. This is not possible in Templin as it does not pertain to peer-to-peer networks, and accordingly does not disclose a P2P server. This is also not possible in Schneider as it only discloses conventional peer-to-peer data transfer, i.e., no interception node.

According to the final office action, Morris discloses querying a P2P server for location information of peer nodes involved in a transfer of files (citing to Morris col. 8, lines 1-9) and based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node (citing to Morris col. 8, lines 10-21). It is respectfully submitted that the cited sections of Morris do not relate to identifying nodes <u>involved in a data transfer</u> as required by claim 15. The cited portions of Morris merely disclose identification of peer nodes that maintain and provide metadata. Morris does not disclose maintenance of records of peer nodes involved in a data transfer.

In paragraph 6, the final office action suggests that Morris teaches both data and meta data transfers citing to Morris col. 8, lines 19-21: "After finishing constructing all the peer node locators with the embedded query in step 218, the peer server 14 provides the peer node locators to the waiting process of step 212." Again, this cited portion of Morris does not disclose anything relating to identifying nodes involved in a data transfer of a file. While the peer nodes in Morris may perform data transfer, claim 15 requires identification of nodes involved in a data transfer of a particular file. That is, given a particular file being transferred by peer-to-peer, Morris does not teach or suggest identification of the peer nodes involved in the transfer of that file.

Furthermore, it is worth pointing out that claim 15 requires the step of querying to be part of the method of transferring the file <u>from the interception node</u>. In Morris, the P2P server provides services to peer nodes, not interception nodes. Therefore, Morris cannot possibly disclose querying of a P2P server in the step of transferring the file from the interception node to the second peer node, especially given that the interception node in the final rejection is a proxy server process.

Therefore, it is respectfully submitted that claim 15 is patentable over the combination of Templin, Schneider, and Morris.

VIII. CLAIMS INVOLVED IN THE APPEAL

Claims 10-15 and 22 are involved in the appeal. These claims involved in the appeal are included in the Appendix submitted herewith.

IX. CONCLUSION

For at least the above reasons, allowance of claims 10-15 and 22 is respectfully requested.

Respectfully submitted,
En-Yi Liao

Dated: **7-19-2007**

Patrick Ben
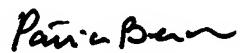
Patrick D. Benedicto, Reg. No. 40,909
Okamoto & Benedicto LLP
P.O. Box 641330
San Jose, CA 95164
Tel.: (408)436-2110
Fax.: (408)436-2114

CERTIFICATE OF MAILING		
I hereby certify that this correspondence, including the enclosures identified herein, is being deposited with the United States Postal Service as first class mail in an envelope addressed to: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on the date shown below. If the Express Mail Mailing Number is filled in below, then this correspondence is being deposited with the United States Postal Service "Express Mail Post Office to Addressee" service pursuant to 37 CFR 1.10.		
Signature: _Patrick Ben_		
Typed or Printed Name: **Patrick D. Benedicto**	Dated:	**July 19, 2007**
Express Mail Mailing Number (optional):		
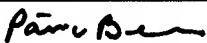
CLAIMS APPENDIX

CLAIMS INVOLVED IN THE APPEAL

10.   A method of transferring a file in a peer-to-peer computer network, the method comprising:

redirecting the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

processing the file in the interception node; and

transferring the file from the interception node to the second peer node.

11.   The method of claim 10 wherein the peer-to-peer computer network includes the Internet.

12.   The method of claim 10 wherein processing the file in the interception node comprises scanning the file for viruses.

13.   The method of claim 10 wherein processing the file in the interception node comprises filtering a content of the file.

14.   The method of claim 10 wherein redirecting the file comprises:

informing the second peer node that an address of the first peer node is that of the interception node.

15.   The method of claim 10 wherein transferring the file from the interception node to the second peer node comprises:

querying a P2P server for location information of peer nodes involved in a transfer of the file;

based on a response from the P2P server, identifying the second peer node as a node involved in the transfer of the file from the first peer node; and

transferring the file from the interception node to the second peer node.

22.   A method of transferring a file in a peer-to-peer computer network, the method comprising:

transferring the file from a first peer node to an interception node, the file being originally intended to be transferred directly from the first peer node to a second peer node, the first peer node and the second peer node being computers in the peer-to-peer computer network;

scanning the file for viruses in the interception node; and

transferring the file from the interception node to the second peer node.

EVIDENCE APPENDIX

There are no documents or items submitted under this section.

RELATED PROCEEDINGS APPENDIX

There are no documents or items submitted under this section.